

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

Overview

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale, and importation of Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software, and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 10,609,063 (the "'063 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '063 Patent by providing its customers and others the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials, and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**




10,609,063 Claim 10	Evidence
<p>A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:</p>	<p>ManageEngine includes <i>a non-transitory computer-readable media storing instructions that, when executed by one or more processors</i> (e.g., the system on which the management software is operated)</p> <p>Note: See, for example, the evidence below (emphasis added, if any):</p> <div data-bbox="751 553 1703 1252"> <p style="text-align: center;">Enterprise vulnerability management software</p> <p style="text-align: center;">Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step vulnerability management in your enterprise with Vulnerability Manager Plus.</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <p>Scan</p>  <p>Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices.</p> </div> <div style="text-align: center;"> <p>Assess</p>  <p>Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker.</p> </div> <div style="text-align: center;"> <p>Manage</p>  <p>Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing.</p> </div> </div> </div> <p>https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&loc=ProdMenu&cat=UEMS</p>

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

Comprehensive vulnerability scanning

Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:

- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

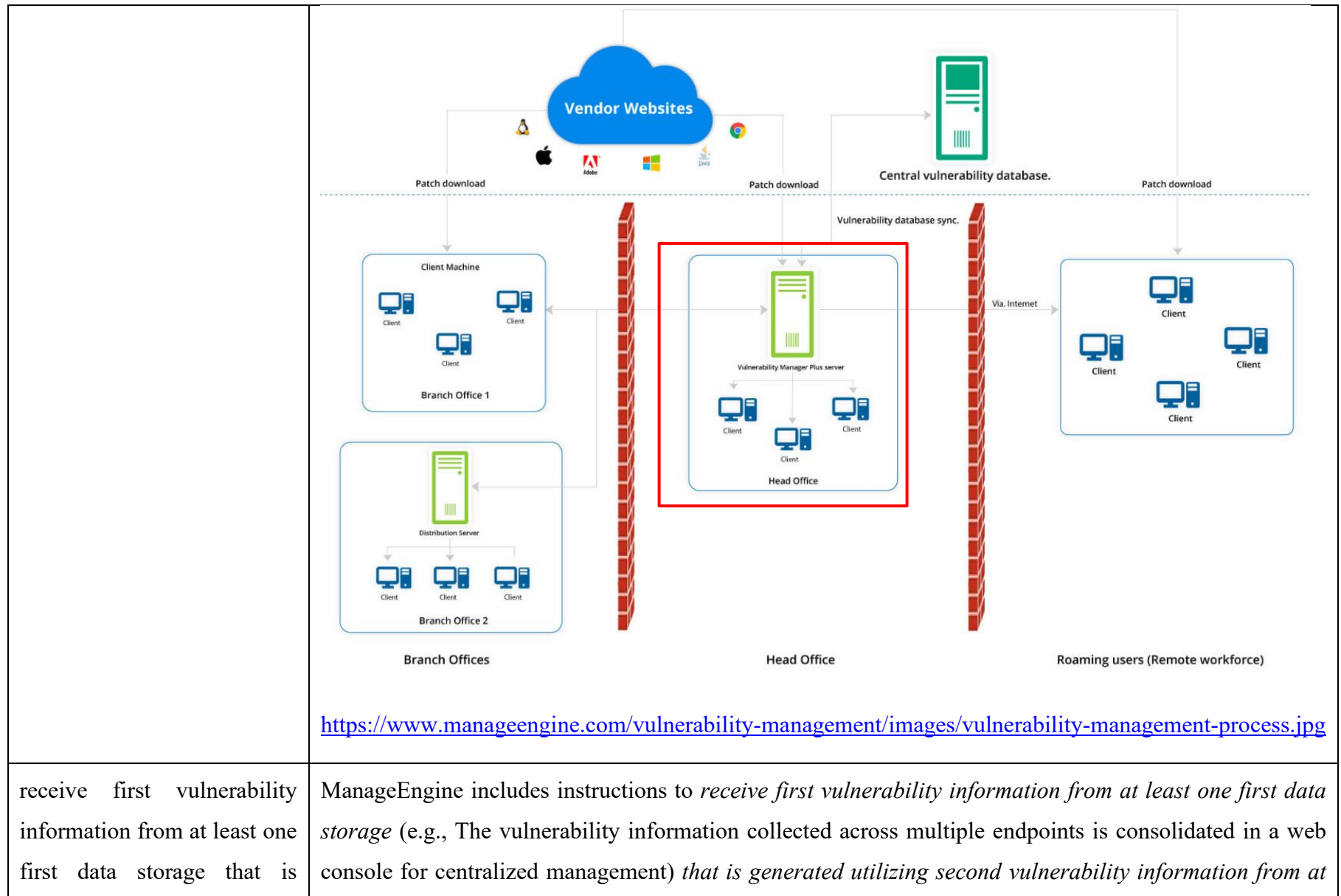
EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

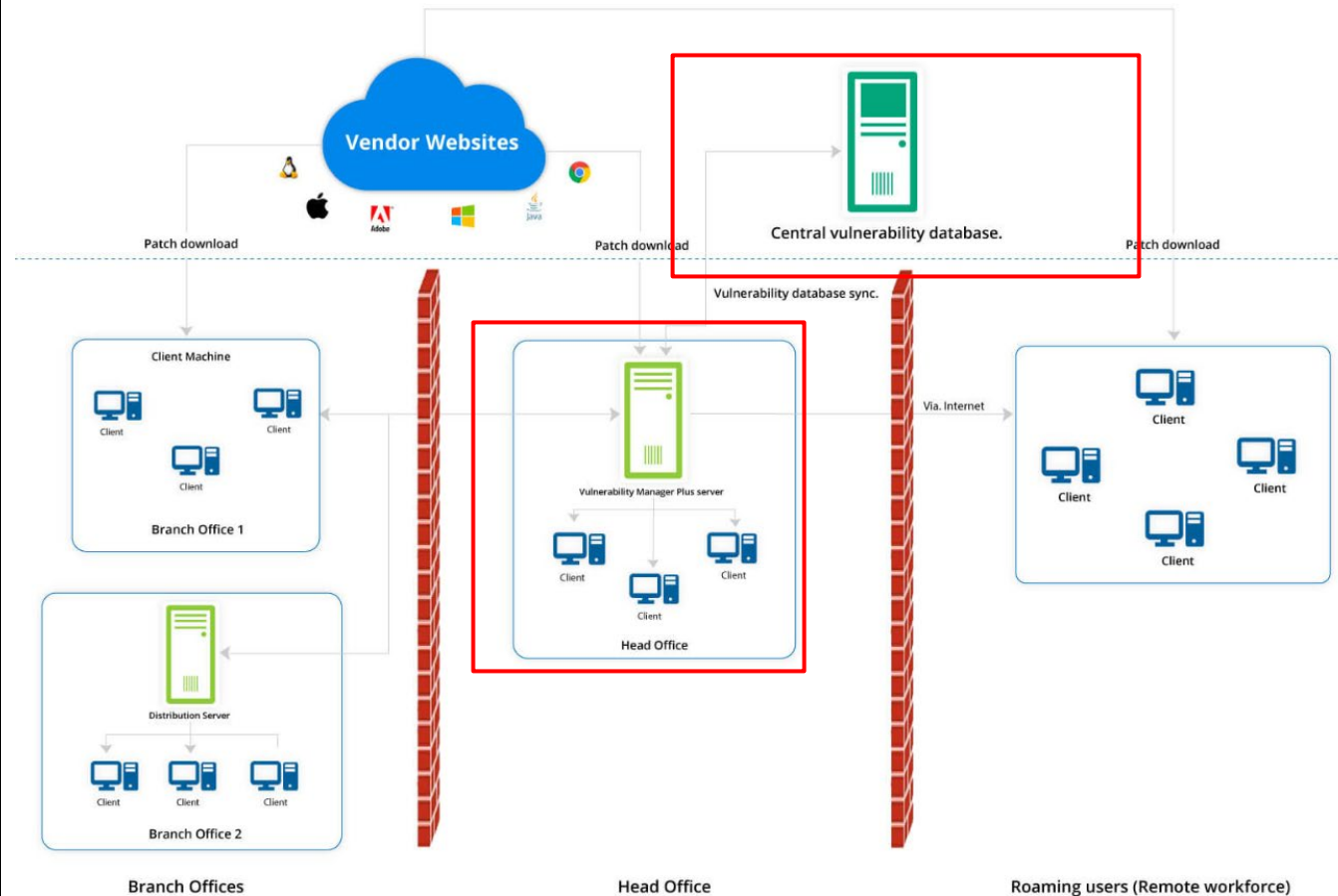
EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

<p>generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;</p>	<p><i>least one second data storage</i> (e.g., a Central Vulnerability Database) <i>that is used to identify a plurality of potential vulnerabilities</i> (e.g., a Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Vulnerability Manager Plus Server:</p> <p>The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following:</p> <ul style="list-style-type: none"> • Installing agents in computers • Scanning computers for vulnerabilities and misconfigurations • Deploying patches and secure configurations • Uninstalling high-risk software • Auditing active ports • Auditing for compliance against CIS benchmarks <p>Any of the Windows computers in your network with the requirements mentioned here can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth.</p>
--	---

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

<https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html#v1>



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary


Zero-day
vulnerabilities

Vulnerability
Age Matrix

Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities		Vulnerable Software			
Vulnerabilities		Affected Systems	Exploit Status	Software Name	
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	1	Available	Windows 8.1 Enterprise Edition (x64)	
				Windows 8.1 Home Basic Edition (x64)	
				Windows 8.1 Home Premium Edition (x64)	
				Windows 8.1 Professional Edition (x64)	

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The top navigation bar includes links for Dashboard, Threats, Patches, Deployment, Systems, Reports, Agent, Admin, and Support. The left sidebar shows a tree view with categories like Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area is titled 'Threats' and includes a filter by 'Threat Category' and a search bar. A table lists vulnerabilities with columns for Threats, Threat Category, Affected Systems, and Action. The table shows five entries, including Google Chrome (x64) and various Internet Explorer security updates. The bottom right of the table indicates '1 - 5 of 5' and a page size of '30'.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675CVE-2019-1255	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675CVE-2019-1255	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

<p>said first vulnerability information generated utilizing the second vulnerability information, by:</p> <p>identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and</p> <p>determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;</p>	<p>ManageEngine includes instructions to receive <i>first vulnerability information generated utilizing the second vulnerability information</i> (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and is generated using information available on a Central Vulnerability Database) <i>identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device</i> (e.g., The vulnerability information collected across multiple endpoints). <i>determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities</i> (e.g., scan the system on the basis of the vulnerability definition stored on Central Vulnerability Database)</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>
--	--

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus interface. The top navigation bar includes links for Dashboard, Threats, Patches, Deployment, Systems, Reports, Agent, Admin, and Support. The left sidebar lists various threat categories, with 'Zero-day Vulnerabilities' highlighted. The main content area displays a table of zero-day vulnerabilities. The table has columns for Threats, Threat Category, Affected Systems, and Action. The first row shows 'Google Chrome (x64) (78.0.3904.87)' with a threat category of 'ZeroDay_CVE-2019-13721_6_CVE-2019-...' and one affected system. The second row shows '2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...' with a threat category of 'CVE-2019-13675CVE-2019-1255' and one affected system. The third row shows '2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...' with a threat category of 'CVE-2019-13675CVE-2019-1255' and one affected system. The fourth row shows '2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...' with a threat category of 'IE_ZeroDay_CVE-2018-8653' and one affected system. The fifth row shows '2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...' with a threat category of 'IE_ZeroDay_CVE-2018-8653' and one affected system. The table also includes a 'Fix' button for each row. The bottom right corner of the table shows '1 - 5 of 5' and a '30' value.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675CVE-2019-1255	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675CVE-2019-1255	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

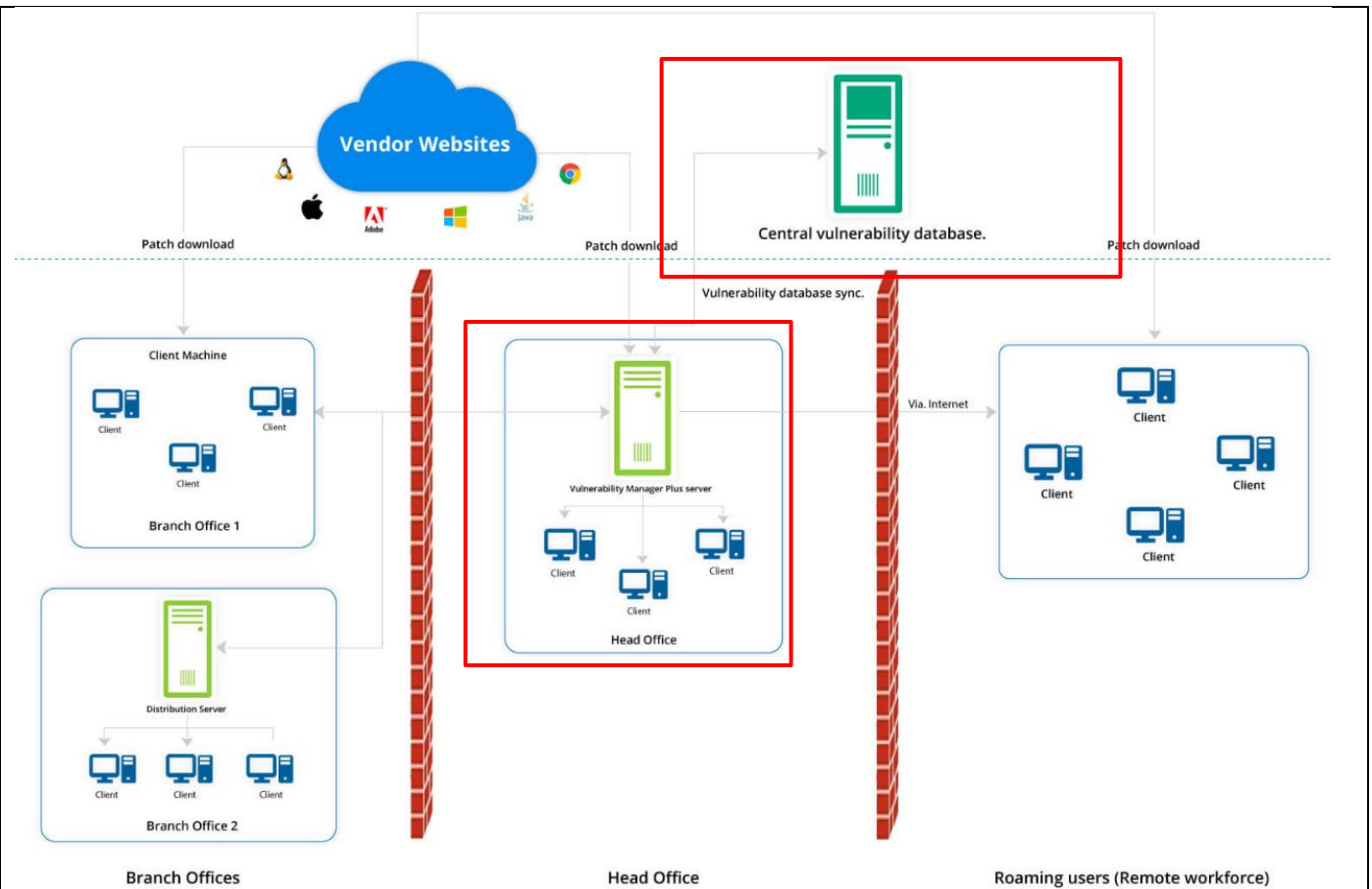
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary


Zero-day
vulnerabilities

Vulnerability
Age Matrix

Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities		Vulnerable Software	
Vulnerabilities		Affected Systems	Exploit Status
			Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
	1	Available	Windows 8.1 Home Basic Edition (x64)
	1	Available	Windows 8.1 Home Premium Edition (x64)
	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

display information that is based on the first vulnerability information;	<p>ManageEngine includes instructions to display <i>information that is based on the first vulnerability information</i> (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management)</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>
---	---

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

	<div><div>See what matters most at a glimpse with dashboard widgets</div><div>The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results. These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.</div><div><div><div>Vulnerability Severity Summary</div><div>Zero-day vulnerabilities</div><div>Vulnerability Age Matrix</div><div>Vulnerabilities Over Time</div><div>High Priority Vulnerabilities</div></div><div><div>High Priority Vulnerabilities: Where your primary focus should be!</div><div><div><div>VulnerabilitiesVulnerable Software</div><div><div>View More</div></div><table><thead><tr><th>Vulnerabilities</th><th>Affected Systems</th><th>Exploit Status</th><th>Software Name</th></tr></thead><tbody><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Enterprise Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Home Basic Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Home Premium Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Professional Edition (x64)</td></tr></tbody></table></div></div><div><div>Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.</div><div>https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html</div></div></div></div></div>	Vulnerabilities	Affected Systems	Exploit Status	Software Name	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)
Vulnerabilities	Affected Systems	Exploit Status	Software Name																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)																		
cause utilization of different occurrence mitigation actions of diverse occurrence	ManageEngine includes instructions to cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type (e.g., ManageEngine Vulnerability Manager Plus includes firewall option), an intrusion mitigation system-based																				

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

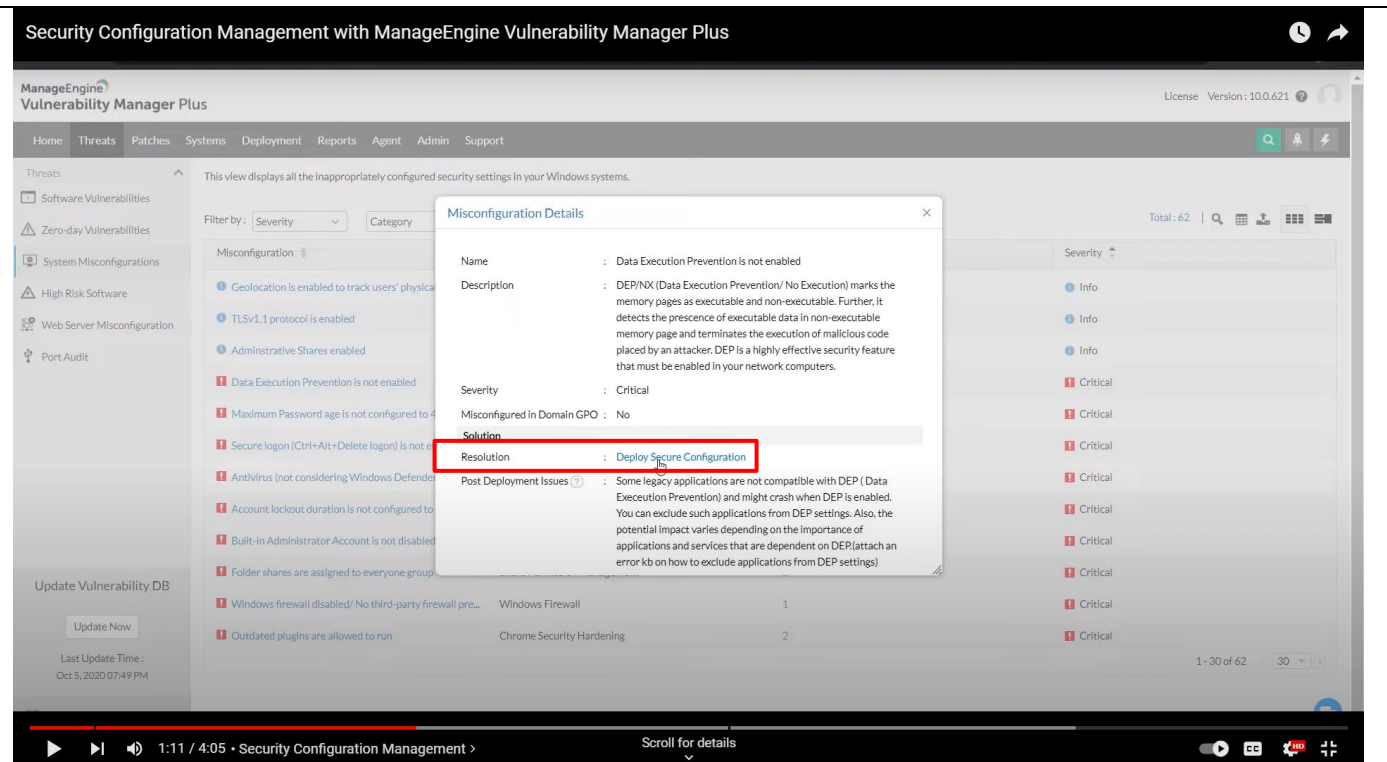
<p>mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and</p>	<p><i>occurrence mitigation type</i> (e.g., ManageEngine Vulnerability Manager Plus includes antivirus option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements. Further, <i>across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices</i> (e.g., ManageEngine Vulnerability Manager Plus includes firewall option and the agent on each installed endpoint will actively scan the device details and remediated by deploying available remediation.). ManageEngine Vulnerability Manager Plus provide option to deploy patches and configuration from central dashboard.</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>
--	---

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations (selected), High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area shows a list of system misconfigurations. A dropdown menu for 'Category' is open, with 'Windows Firewall' highlighted. The table below lists various misconfigurations, their categories, affected systems, and severity levels. Two entries are highlighted with red boxes: 'Windows Firewall' in the category dropdown and the entry 'Windows firewall disabled/ No third-party firewall pre...' in the table.

Misconfiguration	Category	Affected Systems	Severity
Geolocation is enabled to track	User Account Management	2	Info
TLSv1.1 protocol is enabled	Windows Firewall	1	Info
Administrative Shares enabled	Password Policy	3	Info
Data Execution Prevention is r	SSL and TLS Security	4	Critical
Maximum Password age is not configured to 45 days	Chrome Security Hardening	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Security Hardening	1	Critical
Antivirus (not considering Windows Defender) not inst...	Password Policy	1	Critical
Account lockout duration is not configured to 1440 mi...	Logon Security	2	Critical
Built-in Administrator Account is not disabled	Antivirus Protection	2	Critical
Folder shares are assigned to everyone group	Logon Security	2	Critical
Windows firewall disabled/ No third-party firewall pre...	User Account Management	1	Critical
Outdated plugins are allowed to run	Share Permission Management	2	Critical
	Windows Firewall	1	Critical
	Chrome Security Hardening	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

<https://www.youtube.com/watch?v=p20h87NruMo&t=53s>

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the 'Firewall Rule Administration' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the ManageEngine Vulnerability Management console. The left sidebar contains navigation links: Home, Threads, Patches, Systems, Deployment, Agent, Reports, Admin, and Support. The main content area is titled 'Install Universal Windows Patch (Computer)'. It includes a 'Name and Description' section with a text input field containing 'MSConfiguredP02' and an 'Add Description' link. Below this is the 'Install Patch' section, which shows a table of patches. The table has columns for Patch ID, Patch Description, Patch Type, Patch Type, Approval Status, Missing Systems, Installed Systems, and Action. Two patches are listed: '10300' and '10304', both for 'Security Updates for Windows 10 KB5013700' and 'Security Updates for Windows 10 KB5013700' respectively. The 'Approval Status' for both is 'Approved'. The 'Missing Systems' column shows '1' for both, and the 'Installed Systems' column shows '0'. The 'Action' column has a 'X' icon for both. Below the table is the 'Scheduler Settings (optional)' section, which includes checkboxes for 'Install on first' and 'Do not apply this configuration after the time specified below'. The 'Deployment Rule' section has a checkbox for 'Continue deployment even if patches are not installed'. The 'Deployment Settings' section has a dropdown for 'Apply Deployment Policy' set to 'Select Policy' and a 'Create New Policy' link. The 'Define Target' section has a 'Target' dropdown set to 'Remote Office/Domain' and a 'Local Office' dropdown set to 'Local Office'. The 'Filter Computers based on' dropdown is set to 'Computer' and the 'Exclude Target' dropdown is set to 'Select'. The 'Execution Settings (Optional)' section is at the bottom.

Patch ID	Patch Description	Patch Type	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
10300	Security Updates for Windows 10 KB5013700	MS-Require	Security Updates	Approved	1	0	X
10304	Security Updates for Windows 10 KB5013700	MS-Require	Security Updates	Approved	1	0	X

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices utilizing one or more monitors;	<p>ManageEngine <i>receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices utilizing one or more monitors</i> (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management)</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>
--	---

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot displays the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar shows a navigation menu with options like 'Threats', 'Software Vulnerabilities', 'Zero-day Vulnerabilities', 'System Misconfigurations', 'High Risk Software', 'Web Server Misconfiguration', and 'Port Audit'. The main content area is titled 'Threats' and includes a sub-header: 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' Below this, there is a search bar and a table of vulnerabilities. The table has columns for 'Threats', 'Threat Category', 'Affected Systems', and 'Action'. The table lists several vulnerabilities, including Google Chrome (x64) and various Internet Explorer security updates. The 'Action' column for each entry contains a 'Fix' button. At the bottom right of the table, it shows '1 - 5 of 5' and a '30' value.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721&CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675&CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675&CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 11**U.S. Patent No 10,609,063 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results. These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix





Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

<p>wherein the at least one configuration involves at least one operating system.</p>	<p>ManageEngine includes <i>least one configuration involves at least one operating system</i> (e.g., ManageEngine Vulnerability Manager Plus includes operating system information).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Comprehensive vulnerability scanning</p> <p>Eliminating blind spots is the basis of successful vulnerability management. To achieve this, Vulnerability Manager Plus:</p> <ul style="list-style-type: none"> • Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems. • Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move. • Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more. <p>https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html</p>
---	--

EXHIBIT 11

U.S. Patent No 10,609,063 v. Zoho

You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.

Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.

Generally, patches are downloaded directly from vendor sites, stored centrally in the server's patch store, and replicated to your network endpoints to conserve bandwidth. For remote workers, you can have the client machines download essential patches from trusted vendor sites without bottlenecking the limited bandwidth of the VPN gateways.

The web console is the heart of vulnerability management. It allows you to monitor your security posture and carry out all tasks anywhere, anytime.

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>